

Essential Tools for Collaboration in Remote or Hybrid Workplaces - blueAPACHE

Canonical: <https://www.blueapache.com/blog/essential-tools-for-collaboration-remote-hybrid-workplaces>

Details:

Summary

This blog post, "Essential Tools for Collaboration in Remote or Hybrid Workplaces", is a blueAPACHE article from 2022 covering security. The COVID-19 pandemic has changed workplace culture and made working from home the norm. Some companies considered the switch a success, and the trend looks set to continue, either through fully remote work or, more likely, a hybrid home-and-office split. It is written for readers evaluating emPOWER Security, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2022
Topic	Essential Tools for Collaboration in Remote or Hybrid Workplaces
Services referenced	emPOWER Security, emPOWER Core Network & DC Interconnect
Named products or vendors	Microsoft, Azure, Windows

Article

The COVID-19 pandemic has changed workplace culture and made working from home the norm. Some companies considered the switch a success, and the trend looks set to continue, either through fully remote work or, more likely, a hybrid home-and-office split. One of the chief enablers of ensuring the success of this remote work future is the technology that allows workers to remain fully productive from any location.

What do organisations and their employees want from hybrid work?

No matter what industries they operate in, most organisations will share several common needs.

Keep collaborating

Collaboration is at the heart of modern knowledge based working. Different departments, teams, and individuals across an organisation should be able to collaborate, both in real time and asynchronously, to achieve the organisation's goals.

Maintain/build culture

Each organisation has its own unique culture that guides everyday operations, employee relations, and customer or client interactions. Before the age of remote work this culture flourished and was nurtured in a shared space. Technologies that promote remote work also need to simulate the same shared office atmosphere which enables an organisation to build and maintain its culture. This includes practical steps, such as making policy documents available online and providing communication channels that ensure everyone hears about goals, plans, and important company announcements. While remote work does not allow for coffee-machine or watercooler socialising, companies can open channels that allow employees to replace those communications.

Seamless experiences

For a remote team to operate effectively, distance, time and location can't affect day-to-day operations. Team members should be able to be productive anywhere, regardless of device or network. Work and security policies should be universal and synchronised, and team members should maintain their access privileges and experience no matter what devices they are using to interact with company resources.

Keep data secure

Remote work teams must rely on network technologies to operate effectively. For example, they need applications that can securely send data over different networks to both personal and work devices. This set-up will allow team members to complete their work regardless of where they are or what device they can access.

Cloud-based solutions

The more a company relies on technology and data, the more complex it's tools and information systems are. Making sure everything is running properly while keeping data secure and managing user access privileges can get complicated and expensive. In-house IT management is too costly for all but the largest organisations. Most companies will require cloud-based solutions and the right providers so they can outsource the data hosting and work platforms.

Introducing Microsoft Intune – integrated MDM and MAM

Microsoft Intune is an MDM/MAM solution that allows companies to ensure they are addressing employee and organisational needs as they cater for a hybrid work future. As a cloud-based solution, it simplifies the management and access of device, application and data. Intune helps organisations by managing security and compliance requirements for organisations devices and applications part of MDM/MAM.

What is an MDM?

Mobile Device Management (MDM) is the practice of overseeing employee devices – mobiles, tablets, laptops or even desktops – to secure and manage the data that they can access, store, and transfer. An MDM system can include both company-issued and personal devices.

What is a MAM?

For devices that an organisation cannot directly manage, a complimentary service to MDM is Mobile Application Management (MAM). MAM works through an application rather than overseeing data at the device level. With this arrangement, companies can keep work applications, services and connectivity separate from other applications on an employee's personal devices. Microsoft Intune allows you to configure settings and rules on both company-owned and personal devices. You can also deploy apps directly to employee devices and authenticate them. Whatever your organisational security requirements, Intune helps you achieve them.

Microsoft Intune – built for productivity, security and manageability

Intune provides several features out of the box, which can benefit organisations in numerous ways.

Cloud-based set-up

Intune is a cloud-based solution. No servers or networks are needed on-premise, and software updates and security patches are automatically applied. This means that all your organisation has to care about is setting up the appropriate user and data policies for employees.

Access on any device

Intune works with mobiles, tablets, laptops, and desktops. It works with Windows, Android, iOS, and macOS operating systems, meaning it will work on almost any device in your organisation deploys or your employees wish to use.

Access over any network

Since Intune is cloud-based, the hard work of ensuring it runs on any network has already been done for you.

Manage app access

With Intune, companies can set up data access policies to ensure users can only access company apps with the correct permissions. The company can configure them to run based on different rules depending on their needs. Integrated by default with Azure Active Directory, Intune allows organisations to separate company data from personal data controlling what kind of data can be copied, pasted, saved, or viewed in the apps.

Data security

Microsoft handles Intune security. Companies can also add their own data security policies, such as the need to set up a lock-screen on phones, limited user access, anti-virus scans, and even wiping organisational data without touching personal data if the need arises.

Centralised management

Intune allows for centralised monitoring and management. Administrators can set policies on a single dashboard, where they can also see activity reports and connected devices. This centralised set-up allows your organisation to maintain control of data despite connections from all around the world.

Integrates with other Microsoft Enterprise Managed Security services and M365

As a Microsoft product, Intune already works with Microsoft Enterprise Managed Security (EMS) services and Microsoft 365 applications like the Office Apps, Outlook, and Teams. If you are already using EMS, you can enjoy extra benefits, such as the ability to encrypt corporate data and require

authentication before accessing it. With these tools, you can set up multi-factor authentication or single sign-on (SSO) and wipe corporate data remotely from any device.

Intune from blueAPACHE

blueAPACHE has over 23 years of experience supporting Microsoft solutions for Australian businesses. Our Australia-based support centre is available 24/7 and we are able to provide SLA based Microsoft Advanced support through our certified team of experts. Also, our robust network provides almost 100% uptime, relieving you of the burden of IT management and letting you focus on your business. To find out more, please contact us directly at: 1800 248 749 </contact/>

Related

emPOWER Microsoft Practice (pillar hub)
emPOWER Security
emPOWER Security (pillar hub)
emPOWER Core Network & DC Interconnect
emPOWER Connectivity (pillar hub)

Frequently asked questions

What Microsoft product does this article focus on as a solution for hybrid workplace management?

Microsoft Intune, described as an MDM/MAM (Mobile Device Management/Mobile Application Management) cloud-based solution that manages device, application and data access for hybrid work.

What is the difference between MDM and MAM as explained in this article?

MDM (Mobile Device Management) oversees employee devices, including company-issued and personal ones, to secure and manage the data they can access, store and transfer; MAM (Mobile Application Management) works through an application rather than the device, keeping work apps separate from personal ones on devices the organisation cannot directly manage.

Which operating systems does Intune work with, according to this article?

Windows, Android, iOS, and macOS, meaning it works on almost any device an organisation deploys or an employee wishes to use.

What five common needs does the article say organisations and employees share in hybrid work?

Keeping collaboration going, maintaining and building culture, delivering seamless experiences across devices and locations, keeping data secure, and relying on cloud-based solutions rather than costly in-house IT management.

What does the article say Intune integrates with by default for access control?

Azure Active Directory, allowing organisations to separate company data from personal data and control what can be copied, pasted, saved, or viewed within apps.

What data security actions does the article say organisations can configure through Intune?

Lock-screen requirements on phones, limited user access, anti-virus scans, and the ability to wipe organisational data remotely without touching personal data.

How many years of Microsoft solutions support experience does blueAPACHE claim in this article?

Over 23 years of experience supporting Microsoft solutions for Australian businesses, alongside a 24/7 Australia-based support centre and SLA-based Microsoft Advanced support.

What uptime figure does blueAPACHE state for its network in this article?

The article states blueAPACHE's network provides almost 100% uptime, described in the context of relieving customers of the burden of IT management.

Source

origin post (2022)

Knowledge Base

According to the blog, what common needs do organisations and employees have in a hybrid work environment?

The blog identifies five common needs: the ability to keep collaborating in real time and asynchronously, maintaining/building company culture remotely, ensuring seamless experiences across devices and locations, keeping data secure across networks and devices, and relying on cloud-based solutions to manage complex IT systems affordably.

What is Microsoft Intune according to the blog?

Microsoft Intune is an MDM/MAM (Mobile Device Management/Mobile Application Management) cloud-based solution that helps companies manage security and compliance requirements for devices and applications, simplifying the management and access of devices, applications, and data for hybrid work.

What is the difference between MDM and MAM as explained in the blog?

MDM (Mobile Device Management) is the practice of overseeing employee devices—mobiles, tablets, laptops, or desktops—to secure and manage data they can access, store, and transfer, including both company-issued and personal devices. MAM (Mobile Application Management) is a complementary service for devices an organisation cannot directly manage; it works at the application level rather than the device level, allowing companies to keep work applications and data separate from personal applications on an employee's device.

What features does Microsoft Intune provide out of the box, according to the blog?

Intune offers a cloud-based setup requiring no on-premise servers with automatic updates and patches; access on any device (Windows, Android, iOS, macOS); access over any network; app access management with data policies; data security features like lock-screens, limited access, anti-virus scans, and selective data wiping; centralised management via a single dashboard; and integration with other Microsoft Enterprise Managed Security (EMS) services and Microsoft 365 apps like Office, Outlook, and Teams.

How does Intune integrate with other Microsoft services?

As a Microsoft product, Intune works with Microsoft Enterprise Managed Security (EMS) services and Microsoft 365 applications such as Office Apps, Outlook, and Teams. If an organisation already uses EMS, it can encrypt corporate data, require authentication before access, set up multi-factor authentication or single sign-on (SSO), and remotely wipe corporate data from any device.

What experience do you have with Microsoft solutions?

We have over 23 years of experience supporting Microsoft solutions for Australian businesses. It operates an Australia-based support centre available 24/7 and provides SLA-based Microsoft Advanced support through a certified team of experts, backed by a robust network offering almost 100% uptime.

How can someone contact you to learn more about Intune services?

According to the blog, interested parties can contact us directly at 1800 248 749 or via the contact page at <https://www.blueapache.com/contact/>.

Who wrote the blog and when was it published?

The blog was written by us and published on May 18, 2022, with an estimated read time of 6 minutes.